МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

# ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»

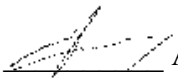
Квалификация (степень) выпускника: Бакалавр

**Кострома**

Рабочая программа дисциплины «Техническая защита информации» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность, утвержден 01.12.2016 г.

Год начала подготовки 2017

Разработал:  Щекочихин Олег Владимирович, к.т.н., доцент, заведующий кафедры защиты информации

Рецензент:  Алексеев Дмитрий Станиславович, доцент кафедры защиты информации, к.т.н.

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _11_ от _30.05.2019_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _8_ от _6.04.2020_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _6_ от _22.01.2021_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

## 1. Цели и задачи освоения дисциплины

**Целями дисциплины** «Техническая защита информации» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»; ознакомление бакалавров с техническими средствами защиты информации (от утечки за счет акустического канала, от виброакустической разведки, от утечки за счет ПЭМИН, от утечки за счет высокочастотного облучения, от утечки за счет каналов сотовой и беспроводной связи, от утечки за счет наводок, стирания информации на носителях); ознакомление с техническими средствами в защищенном исполнении; ознакомление с системами оценки защищенности информации; ознакомление с поисковым оборудованием; ознакомление с техническими средствами экранирования сооружений.

Предмет курса - объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные ресурсы и информационные технологии, в условиях существования угроз в информационной сфере; технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах; процессы управления информационной безопасностью защищаемых объектов.

Профессиональные цели курса - формирование знаний в области принципов добывания (разведки) информации, способов технической защиты информации, активных и пассивных способов и средств скрытия и защиты, способов и средств технической дезинформации, принципов технического контроля защищенности объектов.

Задачи дисциплины:

- изучение систем и средств инженерно-технической разведки, методов и способов организации защиты объектов активными и пассивными способами и техническими средствами, выбора оптимальных (по условиям эксплуатации и экономичности) технических средств защиты информации,
- изучение нормативно-методических и правовых документов, регламентирующих вопросы технической защиты информации;
- формирование умения выявлять каналы утечки на конкретных объектах и оценивать их возможности;
- формирование умения определять рациональные меры защиты на объектах и оценивать уровень эффективности их защиты;
- формирование владения:

- методами организации защиты объектов активными и пассивными способами и техническими средствами;
- методами выбора оптимальных (по условиям эксплуатации и экономичности) технических средств защиты информации;
- методами работы с техническими средствами контроля безопасности информации;
- методами выбора и поиска технических решений защиты объектов информации.

## 2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

**знать**

- принципы и методы технической защиты информации;
- технические каналы утечки информации;
- возможности технических разведок;
- способы и средства защиты информации от утечек по техническим каналам;
- формы и способы представления данных в персональном компьютере;

- физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем;
- универсальные приемы исследования оптимизационных проблем при различной степени неопределенности условий;

**уметь**

- анализировать и оценивать угрозы информационной безопасности объекта;
- пользоваться нормативными документами по защите информации;
- анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности;
- решать типовые прикладные физические задачи;
- применять нормативные документы по метрологии, стандартизации и сертификации на практике;

**владеть**

- методами и средствами выявления угроз безопасности автоматизированным системам;
- методами технической защиты информации;
- методами формирования требований по защите информации;
- методами расчета и инструментального контроля показателей технической защиты информации;
- навыками обеспечения безопасности информации с помощью типовых программных и технических средств;
- навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.

освоить компетенции:

- способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);
- способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2).
- способность проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики (ПСК-2.1);
- способность формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов (ПСК-2.2);
- способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение (ПСК-2.3);
- способность организовать контроль защищенности объекта в соответствии с нормативными документами (ПСК-2.4).

## 3. Место дисциплины в структуре ОП ВО

Дисциплина «Техническая защита информации» относится к циклу базовых дисциплин. Дисциплина формирует представление о защите информации, заключающейся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Дисциплина изучается на третьем курсе, требования к входным знаниям, умениям и навыкам определяются требованиями к уровню подготовки по дисциплине «Математический анализ», «Линейная алгебра», «Физика», «Основы информационной безопасности».

Изучение дисциплины является основой для освоения последующих дисциплин/практик: «Программно-аппаратные средства защиты информации», «Технические средства охраны и видеонаблюдения, «Программно-аппаратные средства защиты информации», «Аудит защищенности объектов информатизации».

## 4. Объем дисциплины (модуля)

### 4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

| Виды учебной работы, | Очная форма |
|---|---|
| Общая трудоемкость в зачетных единицах | 4 |
| Общая трудоемкость в часах | 144 |
| Аудиторные занятия в часах, в том числе: | 68 |
| Лекции | 34 |
| Практические занятия | - |
| Лабораторные занятия | 34 |
| Самостоятельная работа в часах | 40 |
| Форма промежуточной аттестации | экзамен |

### 4.2. Объем контактной работы на 1 обучающегося

| Виды учебных занятий | Очная форма |
|---|---|
| Лекции | 34 |
| Практические занятия | - |
| Лабораторные занятий | 34 |
| Консультации | 0,9 |
| Зачет/зачеты | - |
| Экзамен/экзамены | 36 |
| Курсовые работы | - |
| Курсовые проекты | – |
| Всего | 104,9 |

## 5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий

### 5.1 Тематический план учебной дисциплины

| № п/п | Название раздела, темы | Всего з.е/час | Аудиторные занятия | | Самостоятельная работа |
|---|---|---|---|---|---|
| | | | Лекции | Лабораторные | |
| 1. | Введение. Технические средства защиты информации. | 16 | 6 | 6 | 4 |
| 2. | Технические средства в защищенном исполнении. | 6 | 2 | 2 | 2 |
| 3. | Системы оценки защищенности информации. | 24 | 6 | 8 | 10 |
| 4. | Поисковое оборудование. | 20 | 6 | 6 | 8 |
| 5. | Технические средства экранирования сооружений. | 10 | 2 | 2 | 6 |

| № п/п | Название раздела, темы | Всего з.е/час | Аудиторные занятия | | Самостоятельная работа |
|---|---|---|---|---|---|
| | | | Лекции | Лабораторные | |
| 6. | Программные средства защиты информации. | 32 | 12 | 10 | 10 |
| **Экзамен** | | 36 | | | |
| **Всего:** | | **144** | **34** | **34** | **40** |

**5.2. Содержание:**

**1. Введение. Технические средства (ТС) защиты информации.**

Изучение нормативной документации по защите информации (ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения») ТС защиты от утечки за счёт акустического канала; ТС защиты от виброакустической разведки; ТС защиты от утечки за счёт ПЭМИН; ТС защиты от утечки за счёт высокочастотного облучения (ВЧО); ТС защиты от утечки за счёт каналов сотовой и беспроводной связи; ТС защиты от утечки за счёт наводок; ТС стирания информации на носителях.

**2. Технические средства в защищенном исполнении.**

Защищенные сотовые телефоны. Защищенные абонентские пункты.

**3. Системы оценки защищенности информации.**

Системы оценки защищённости АВАК. Системы оценки защищенности канала ПЭМИН. Системы оценки защищённости канала АЭП. Системы оценки защищённости канала ВОЛС. Вспомогательное оборудование.

**4. Поисковое оборудование.**

Досмотровое оборудование. Имитаторы сигналов. Индикаторы поля. Комплексы выявления беспроводных средств доступа. Комплексы контроля радиообстановки. Контроль цепей питания ТС. Обнаружители видеокамер. Регистраторы модуляции вторичного излучения. Рентгеновское оборудование. Универсальные поисковые устройства. Нелинейные локаторы.

**5. Технические средства экранирования сооружений.**

Экранированные дверные системы. Экранированные светопрозрачные конструкции. Радиопоглощающие материалы. Фильтры сетевые помехоподавляющие. Безэховые и экранированные камеры. Проходные компоненты. Экранирующие палатки.

**6. Программные средства защиты информации.**

ПО для автоматизации деятельности специальных лабораторий. ПО для контроля защищенности информации. Электронный документооборот. Автоматизация взаимодействия с клиентами. Автоматизация деятельности режимно-секретных подразделений. Комплексные системы автоматизации объектов. ПО для организации учебных процессов.

**6. Методические материалы для обучающихся по освоению дисциплины**

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы.

Обучающемуся важно помнить, что лекция эффективно помогает ему овладеть программным материалом благодаря расстановке преподавателем необходимых акцентов

и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации. Кроме того, во время лекции имеет место прямой визуальный и эмоциональный контакт обучающегося с преподавателем, обеспечивающий более полную реализацию воспитательной компоненты обучения.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков применения методов формирования, организации и поддержки комплекса мер по обеспечению информационной безопасности объекта защиты;
- совершенствование навыков поиска публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента.

**6.1. Самостоятельная работа обучающихся по дисциплине (модулю)**

| № п/п | Раздел (тема) дисциплины | Задание | Методические рекомендации по выполнению задания | Форма контроля |
|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** |
| 1. | Тема № 1 | Усвоить | 1. Изучить технические средства защиты информации. Литература основная [1] | Контрольный опрос |
| 2. | Тема № 2 | Усвоить, приобрести навык | 1. Изучить технические средства в защищенном исполнении. Литература основная [1] | Контрольный опрос |
| 3. | Тема № 3 | Усвоить, приобрести навык | 1. Изучить системы оценки защищенности информации. Литература основная [1] | Контрольный опрос |
| 4. | Тема № 4 | Усвоить, приобрести навык | 1. Ознакомиться с поисковым оборудованием. Литература основная [1] | Контрольный опрос |
| 5. | Тема № 5 | Усвоить, приобрести навык | 1. Изучить технические средства экранирования сооружений. Литература основная [1] | Контрольный опрос |
| 6. | Тема № 6 | Усвоить, приобрести навык | 1. Изучить программные средства защиты информации. Литература основная [1] | Контрольный опрос |

Формой отчетности по данной дисциплине является экзамен. Необходимые условия допуска к экзамену:

- Наличие полного конспекта лекций.
- Сдача всех лабораторных работ с положительным результатом.

**6.2. Тематика и задания для практических занятий (*при наличии*)**

*Не предусмотрены*

**6.3. Тематика и задания для лабораторных занятий**

1. ТС защиты от утечки за счёт акустического канала; ТС защиты от виброакустической разведки; ТС защиты от утечки за счёт ПЭМИН; ТС защиты от утечки за счёт

высокочастотного облучения (ВЧО); ТС защиты от утечки за счёт каналов сотовой и беспроводной связи; ТС защиты от утечки за счёт наводок; ТС стирания информации на носителях.

2. Защищенные сотовые телефоны. Защищенные абонентские пункты.
3. Системы оценки защищённости АВАК. Системы оценки защищенности канала ПЭМИН. Системы оценки защищённости канала АЭП. Системы оценки защищённости канала ВОЛС. Вспомогательное оборудование.
4. Индикаторы поля. Обнаружители видеокамер. Универсальные поисковые устройства. Нелинейные локаторы.
5. Экранированные дверные системы. Экранированные светопрозрачные конструкции. Радиопоглощающие материалы. Фильтры сетевые помехоподавляющие. Безэховые и экранированные камеры. Проходные компоненты.
6. ПО для автоматизации деятельности специальных лабораторий. ПО для контроля защищенности информации. Электронный документооборот. Автоматизация взаимодействия с клиентами. Автоматизация деятельности режимно-секретных подразделений. Комплексные системы автоматизации объектов. ПО для организации учебных процессов.

## 7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

**а) основная**

1. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

**б) дополнительная**

1. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. — М. : РИОР : ИНФРА-М, 2017. — 111 с. — (Научная мысль). — http://znanium.com/catalog.php?bookinfo=854634
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : Учеб. пособие для студ. / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - 2-е изд. - М. : Горячая линия-Телеком, 2004. - 147 с. : ил. - (Учебное пособие для высших учебных заведений). - Библиогр.: с. 143-145. - ISBN 5-93517-062-0 : 45.75. Допущено УМО

## 8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Информационно-образовательные ресурсы:

1. www.atlas.Krasnodar.ru -КФ НТЦ «Атлас»: защита информации.

Электронные библиотечные системы:

1. Университетская библиотека онлайн http://biblioclub.ru
2. «Лань» http://e.lanbook.com/
3. ЭБС «Znanium»
4. Справочно-информационная система (СИС) «Гарант».
5. Справочно-информационная система «Консультант».
6. Электронно-библиотечная система (ЭБС) «Инфра-М».

## 9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционная аудитория, оснащенная проектором, компьютером.

Лаборатория технической защиты информации.